

1        SECURE ANONYMOUS VERIFICATION, GENERATION AND/OR PROOF OF  
2                                OWNERSHIP OF ELECTRONIC RECEIPTS

3                                ABSTRACT

4        A method, apparatus and system is provided for secure  
5        anonymous proof of ownership of electronic receipts, wherein  
6        a sender sends a first message including a transaction  
7        request and referencing an owner of a receipt to be  
8        generated to a first addressee. The first addressee returns  
9        a signed receipt including the reference and details for  
10       what the receipt has been given. The sender sends a signed  
11       second message including the receipt to a second addressee.  
12       The second addressee obtains a public signature verification  
13       key on the basis of the reference to the owner of the  
14       receipt and authenticates the second message. A major  
15       advantage of the invention is that in a pseudonymous or  
16       anonymous transaction based system it is now possible to  
17       remain anonymous or pseudonymous when presenting electronic  
18       receipts, while securely proving ownership of the receipt.